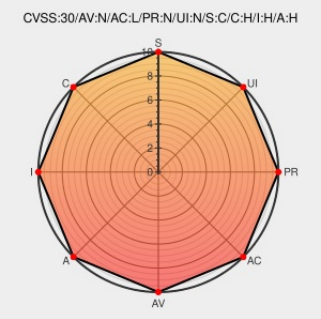
CVE-2019-12643

Published on: 08/28/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:41 PM UTC

CVE-2019-12643 - advisory for cisco-sa-20190828-iosxe-rest-auth-bypass

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of 4221 Integrated Services Router from Cisco contain the following vulnerability:

A vulnerability in the Cisco REST API virtual service container for Cisco IOS XE Software could allow an unauthenticated, remote attacker to bypass authentication on the managed Cisco IOS XE device. The vulnerability is due to an improper check performed by the area of code that manages the REST API authentication service. An attacker could exploit this vulnerability by submitting malicious HTTP requests to the targeted device. A successful exploit could allow the attacker to obtain the token-id of an authenticated user. This token-id could be used to bypass authentication and execute privileged actions through the interface of the REST API virtual service container on the affected Cisco IOS XE device. The REST API interface is not enabled by default and must be installed and activated separately on IOS XE devices. See the Details section for more information.

CVE-2019-12643 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as CRITICAL severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: **Cisco** - **Cisco IOS XE Software** version **16.09.03**

CVSS3 Score: 10 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication

NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20190828 Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	4221 Integrated Services Router	-	All	All	All
Hardware	Cisco	4221 Integrated Services Router	-	All	All	All
Hardware	Cisco	4321 Integrated Services Router	-	All	All	All
Hardware	Cisco	4321 Integrated Services Router	-	All	All	All
Hardware	Cisco	4331 Integrated Services Router	-	All	All	All
Hardware	Cisco	4331 Integrated Services Router	-	All	All	All
Hardware	Cisco	4351 Integrated Services Router	-	All	All	All
Hardware	Cisco	4351 Integrated Services Router	-	All	All	All
Hardware	Cisco	4431 Integrated Services Router	-	All	All	All
Hardware	Cisco	4431 Integrated Services Router	-	All	All	All
Hardware	Cisco	4451-x Integrated Services Router	-	All	All	All
Hardware	Cisco	4451-x Integrated Services Router	-	All	All	All
Hardware	Cisco	Cloud Services Router 1000v	-	All	All	All
Hardware	Cisco	Cloud Services Router 1000v	-	All	All	All
Operating System	Cisco	Ios Xe	15.5(3)s3.16	All	All	All
Operating System	Cisco	Ios Xe	15.5\(3\)s3.16	All	All	All
Operating	Cisco	Ios Xe	16.6.5	All	All	All

System						
Operating System	Cisco	Ios Xe	15.5\(3\)s3.16	All	All	All
Operating System	Cisco	Ios Xe	16.6.5	All	All	All

cpe:2.3:h:cisco:4221_integrated_services_router:-:*:*:*:*:*:*:*:
cpe:2.3:h:cisco:4221_integrated_services_router:-:*:*:*:*:*:*:*:
cpe:2.3:h:cisco:4321_integrated_services_router:-:*:*:*:*:*:*:*:
cpe:2.3:h:cisco:4321_integrated_services_router:-:*:*:*:*:*:*:*:
cpe:2.3:h:cisco:4331_integrated_services_router:-:*:*:*:*:*:*:*:
cpe:2.3:h:cisco:4331_integrated_services_router:-:*:*:*:*:*:*:*:
cpe:2.3:h:cisco:4351_integrated_services_router:-:*:*:*:*:*:*:*:
cpe:2.3:h:cisco:4351_integrated_services_router:-:*:*:*:*:*:*:*:
cpe:2.3:h:cisco:4431_integrated_services_router:-:*:*:*:*:*:*:*:
cpe:2.3:h:cisco:4431_integrated_services_router:-:*:*:*:*:*:*:*:
cpe:2.3:h:cisco:4451-x_integrated_services_router:-:*:*:*:*:*:*:*:
cpe:2.3:h:cisco:4451-x_integrated_services_router:-:*:*:*:*:*:*:*:
cpe:2.3:h:cisco:cloud_services_router_1000v:-:*:*:*:*:*:*:*:
cpe:2.3:h:cisco:cloud_services_router_1000v:-:*:*:*:*:*:*:*:
cpe:2.3:o:cisco:ios_xe:15.5(3)s3.16:*:*:*:*:*:*:*:
cpe:2.3:o:cisco:ios_xe:15.5\(3\)s3.16:*:*:*:*:*:*:*:
cpe:2.3:o:cisco:ios_xe:16.6.5:*:*:*:*:*:*:*:
cpe:2.3:o:cisco:ios_xe:15.5\(3\)s3.16:*:*:*:*:*:*:*:
cpe:2.3:o:cisco:ios_xe:16.6.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report